Terrorism, Radicalization, and Extremism

CS 152 — Trust and Safety

Alex Stamos

Stanford Cyber Policy Center

2026

Acknowledgments

These slides draw on contributions from:

- **Brian Fishman** — Cinder
- **Christopher David** — Neu-Ulm University of Applied Sciences
- **Marten Risius** — Neu-Ulm University of Applied Sciences
- **Mariana Olaizola Rosenblat** — NYU Stern Center for Business and Human Rights
- **Theodora Skeadas** — PhD researcher, King's College London
- **Inga Kristina Trauthig** — Florida International University

Historical Context

Three parts

1. **History** — extremism on the internet isn't new, and neither are the trust & safety efforts to manage it.
2. **What to do?** — defining harm and figuring out what to do about it.
3. **What's changing now?** — new tactics, lowering the competency bar, and whether technology will create new perpetrators.

Framing adapted from Brian Fishman, "Crossroads: Counter-terrorism and the Internet," *Texas National Security Review* (Feb. 2019).

Big Questions

- **How do you define terrorism and hate?**
  - Non-state actors only? What about **state-sanctioned violence**? Can platforms stand up to governments? *Should* they?
- **What should you do when you find it?**
  - If the definition contains imbalances between parties, can platforms avoid putting their finger on the scale? Should they?
- **How do you detect it?**
  - Keywords? Hashes? Classifiers? LLMs?
- **How do you work with governments?**
  - Law-enforcement referrals save lives. They also create real privacy risk and can be abused.

Cf. Fishman, *TNSR* (2019); Byman & Sachs, *Foreign Affairs* 91(5) (2012).

Timeline: terrorism on the internet

Year	Inflection point
1980s	Bulletin boards — mostly American white supremacists, transnational reach
1996	Stormfront — the web era arrives; deplatforming begins
2004	Broadband and cell phones — terrorists become “creators”
2012	“Lone wolves” — jihadis shift to social media; Anwar al-Awlaki
2017	Christchurch — white-supremacist livestream; multilateral turn
2023	October 7 attack and aftermath — definitional crisis returns

1980s — Bulletin Boards

- Mostly **American white supremacists** — aiming for transnational (Canada) impact
- Recreating **voicemail-style** messaging for organizing and recruitment
- Anyone with a home computer and a modem could reach the boards; sysops controlled access via password lists

THE NEW YORK TIMES, FRIDAY, FEBRUARY 15, 1985

Computer Network Links Rightist Groups and Offers 'Enemy' List

By WAYNE KING

Special to The New York Times

HOUSTON, Feb. 14 — An Idaho-based neo-Nazi organization has established a computer-based network to link rightist groups and to disseminate a list of those who it says "have betrayed their race."

One list available from the computer, titled "Know Your Enemy," includes the addresses and telephone numbers of regional offices of the Anti-Defamation League of B'nai B'rith and the offices of the Communist Party U.S.A. It also includes names and addresses of "race traitors" and "informers."

The computer link, called the "Aryan Liberty Net," is sponsored by the Aryan Nations, an organization based in Hayden Lake, Idaho. Law-enforcement officials have tied a splinter group of the organization to several bank and armored-car robberies, armed attacks on Federal officers and the machine-gun slaying of Alan Berg, a Denver talk show host.

'War' on the United States

The splinter group, calling itself by various names, including the Order and the Brüder Schweigen, German for the Silent Brotherhood, was identified by the Federal Bureau of Investigation as the organizational link for several heavily armed individuals who had "declared war" on the United States Government. The Silent Brotherhood maintains that the Government, which it refers to as the "ZOG," for Zionist Occupation Government, has been taken over by Jews, whom the group regards as descendants of Satan who should be exterminated.

The leader of the group, Robert J. Mathews, 31 years old, was killed in December after firing on Federal officers with a submachine gun from a hideaway on Whidbey Island in Puget Sound, Wash. The house was ignited by illumination flares dropped from a helicopter. Mr. Mathews was sought in connection with the wounding of an F.B.I. agent in Seattle and the robbery of a Brink's armored car in northern California.

Federal investigators later determined that the California robbery, in which $3.6 million was taken by a band of up to 17 men who sprayed the truck with an automatic weapon, was conducted to finance a "war" against the Government. The authorities ascribed the same motive to counterfeiting operations they said were conducted by other members of the group.

The Network's Messages

In the wake of the incident at Whidbey Island, Richard Girnt Butler, head of the Aryan Nations, said Mr. Mathews and several other members of the Silent Brotherhood were "former members" of the Aryan Nations. Mr. Butler called Mr. Mathews "a hero."

One message on the Aryan Nations computer network warns: "The older and less active spokesmen for the fold and faith are being replaced by the young lions. These dragons of God have no time for pamphlets or speeches. They are the armed party which is being born out of the inability of white male youths to be heard."

Another entry is a courtroom statement of a California man convicted in 1982 for killing a 17-year-old who informed on right-wing activities.

The statement accuses the "Satanic society" of the United States of "murdering Christians like Gordon Kahl, who you burned in Nebuchadnezzar's oven because he would not bow to your golden Babylonian God and pay your tribute to finance Israel."

Mr. Kahl, a fugitive charged with killing two Federal marshals, was an outspoken member of a tax-protest group. He was killed in June 1983 when a concrete bunker crammed with thousands of rounds of ammunition exploded in a gun battle with the Federal authorities. He shot and killed Sheriff Gene Matthews of Lawrence County, Ark., in that incident. Mr. Kahl attended Aryan Nations functions and has been cited as a "hero and martyr" by the group.

The Government's continuing investigation has expanded to at least six states.

Weapons and a Point System

Investigators have already found caches of weapons, including explosives and automatic weapons, one of which was identifed by ballistics experts as the one used to kill Mr. Berg, who taunted right-wing extremists on his radio show. The authorities also found literature detailing a "point system" to achieve status by killing Federal officials, blacks or Jews.

The Federal authorities have also discovered the names of public officials and others viewed as enemies by rightists.

Late last month, for example, the F.B.I. notified Lieut. Gov. Bill Baxley of Alabama that he might be a target for revenge. Mr. Baxley, when State Attorney General, was responsible for obtaining the extradition of the racist J. B. Stoner for the bombing of Bethel Baptist Church in Birmingham.

The F.B.I. also uncovered threats linked to the Aryan Nations against Morris Dees of Montgomery, Ala., head of the Southern Poverty Law Center. Mr. Dees has filed several suits against the Ku Klux Klan and helped found Klanwatch, a group that monitors the Klan.

The Federal authorities decline to discuss whether they are monitoring the computer network sponsored by the Aryan Nations.

It was set up by Louis Beam, of Dallas, a member of the Ku Klux Klan. It can be reached through telephone numbers in Texas, Idaho and North Carolina, which has an active Klan.

Access Is Restricted

The computer link, which has varying levels of passwords to restrict access, describes itself as "a pro-American, pro-White, anti-Communist network of true believers who serve the one and only God — Jesus, the Christ," and that it is "for Aryan patriots only."

Under a listing of "known ZOG (Zionist Occupational Government) informers," the network lists the names of an F.B.I. informer against the Klan and a man who testified against a Ku Klux Klansman charged with bombing a California radio station.

The informer was killed last summer, and the network exults: "He was blown to pieces on a recent morning, when he opened his mailbox to remove his newspaper. Oh, glorious day!"

An entry called "At Last, Unity" says: "Finally, we are all going to be linked together at one point in time. Imagine, if you will, all the great minds of the patriotic Christian movement linked together and joined into one computer. Imagine any patriot in the country being able to call up and access these minds."

Post Office Sues Magazine

WASHINGTON, Feb. 14 (AP) — The Postal Service filed suit Wednesday to stop Larry C. Flynt, publisher of Hustler magazine, from sending free copies of his publication "or any other pandering advertisement" to members of Congress who did not want them.

New York Times, 1985 — "Computer Network Links Rightist Groups and Offers 'Enemy' List."

1996 — Stormfront and post-organizational extremism

- Stormfront launches on **Beverly Hills Internet (Geocities)** as hosting provider
- After removal, hosting moves to **Russia… and Florida**
- **Louis Beam** (white supremacists) and **Abu Musab al-Suri** (jihadis) articulate **“leaderless resistance”** and **“phantom organization”** — the move from organization to *post-organization*
- **This wasn’t a surprise**: extremists evolved with the rest of society as the internet went mainstream

Louis Beam, US Army veteran and white-supremacist organizer; author of “Leaderless Resistance” (1983, popularized through 1990s).

2004 — Broadband and content distribution

- Broadband and cell phones mean **image and video files travel anywhere**
- Extremists become **“creators”**, not just users
- Distinct **systems for coordination** vs. **systems for content distribution**
- The **Nicholas Berg** beheading video (May 2004) is a seminal event — mass online distribution of high-impact terrorist content

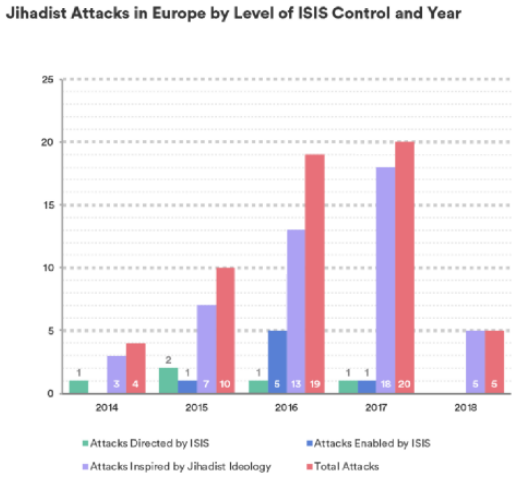
Still from the May 2004 Nicholas Berg video distributed by Abu Musab al-Zarqawi’s network. Image used as a historical artifact; video itself is not shown.

2012 — “Lone wolves” and Anwar al-Awlaki

Anwar al-Awlaki (AFP).

- 2009 attacks push **jihadis onto social-media platforms** — more and more in **English**
- **al-Awlaki** inspires US government to engage platforms; **platforms mostly ignore them**
- The **Syrian civil war and rise of the Islamic State** raise the stakes
- Eventually, engagement starts to work — but only after years of pressure

The lone-actor pattern operationalizes



- By **2017**, nearly all jihadi attacks in Europe are **inspired** rather than **directed**
- *Inspired* = ideology delivered online; attack chosen and executed by the actor alone
- This is **Awlaki's model** operationalizing across an entire ecosystem
- Sets the template that hybrid right-wing and post-Oct.-7 networks now reuse

2017 — Christchurch and the multilateral turn

- Mass shooting at two Christchurch mosques: **51 killed**, livestreamed on Facebook
- **Unprecedented global virality** overwhelms every major platform's takedown capacity
- Inaugurates a more **multilateral** approach — governments, platforms, and civil society:
  - **GIFCT** (Global Internet Forum to Counter Terrorism) hash-sharing
  - **Christchurch Call** to eliminate terrorist and violent-extremist content

2023 — October 7 and the definitional crisis

- October 7, 2023 attacks raise **innumerable definitional questions**:
  - **What counts as terrorism** when there is no global consensus?
  - What is **possible in the face of government pressure**?
  - How do platforms moderate **content from active conflict** at scale?
- Surfaces older arguments about **state-sponsored** and **settler-driven** violence (cf. Byman & Sachs 2012)
- New radicalization pattern: **TikTok-driven, lone-actor**, post-Oct. 7 European cases (Stockhammer, *CTC Sentinel*, July 2025)

Gaza border breach, October 7, 2023.

What's changing now?

- **Encryption** — helps you stay private. Does the same for al-Qaeda, ISIS-K, white-supremacist accelerationists.
- **Artificial intelligence**:
  - If *I* can code now, what will al-Qaeda accomplish?
  - Will **AI-empowered small groups** conduct targeted violence more effectively, more remotely, at lower cost?
  - Will the threat shift toward **tech-focused terrorism** (drones, robotics, autonomous systems)?
- **Will this change *who* is violent?** — AI lowers the competency bar; previously incapable actors gain reach.

Fishman, "AI and the New Blueprint of Terrorism," *War on the Rocks* (Mar. 2026).

Examples: Online Radicalization → Offline Violence

Pride shooting, Oslo — 25 June 2022
"Hateful rhetoric directed at LGBTQ communities and the Pride movement has intensified in recent years, both on closed extremist online forums and on open social media."

Mosque bombing, Peshawar, Pakistan — 30 Jan. 2023
"Terrorist organizations in Pakistan use social media to exploit the vulnerability of youth… by creating fake profiles, sharing photos and videos of attacks."

Religious observers attacked, Bondi Beach, Australia — 14 Dec. 2025
"You've got to try to interrupt people being radicalized, particularly young men, it's the most vulnerable group, and that involves monitoring what is being said online…"

Digital Augmentation of Terrorism and Extremism

Evidence is mixed on whether the internet is a specific risk factor, but online activity plays an integral role in most forms of modern terrorism.

Operational changes:

- Personalizing radicalization approaches; recruiting younger users
- Involving more women (e.g., “Jihadi brides”)
- Dynamically outwitting regulation; fundraising
- Empowering individual actors / lone actors

Structural changes:

- Novel forms of extremist ideology (hybridized, mixed-unclear-unstable)
- Departure from traditional radicalization pathways
- New online threats (doxing, meme warfare, outrage generation)

Binder & Kenyon (2022); Risius et al. (2023).

Defining “Radicalization”

Multiple models and definitions exist:

- **“A process leading towards the increased use of political violence”** — Della Porta & LaFree (2012)
- **“Change in beliefs, feelings, and behaviors in directions that increasingly justify intergroup violence and demand sacrifice in defense of the group”** — McCauley & Moskalenko (2008)
- **“The set of processes that causes attitudinal change that leads towards the use of violence”** — Neumann & Rogers (2007)

→ Radicalization is a **process** that occurs in **opinion** *and* **behavior** — and these can diverge.

Defining “Terrorism”

Several working definitions, no universal one:

- **Behavior-focused**: “premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents” — US Dept. of State
- **Belief-focused**: “a doctrine about the presumed effectiveness of a special form or tactic of fear-generating, coercive political violence” — Schmid (2012)

Implications of lacking a universal definition:

- Politicization and misuse of the term “terrorism”
- Violates *nullum crimen, nulla poena sine lege* (no crime without law)
- Insufficient harmonization between national and regional laws

UNODC (2021); Schmid (2012).

Issues from the lack of a common definition (1/2)

Potential for the weaponization of the term "terrorism":

- Normatively loaded and politically contested
- Places an actor **outside the realm of accepted debate**
- Rarely self-identification; often an **imposed label**

Example: biased use of "terrorism" by the Trump administration

- **Early 2025** — Vandalism against Tesla dealerships framed as "domestic terrorism"
- **Sept. 2025** — Executive order designating left-wing **Antifa** as a "terrorist threat"
- **Early 2026** — Alex Pretti and Renee Good (killed by federal agents in Minneapolis, January 2026) labeled "domestic terrorists" by DHS Secretary Kristi Noem

Issues from the lack of a common definition (2/2)

Excludes state-sponsored violence:

- The Oct. 7, 2023 Hamas attacks intensified debate on **state-sponsored terrorism**
- The Israeli Defense Forces reportedly targeted civilians across Gaza and the West Bank, killing **over 73,188 Palestinians**. Some estimates find 80% of those killed were civilians; 70% of those killed in residential buildings were women and children
- These attacks feed larger conversations on state sponsorship by the United States, Iran, Russia, and others
- Legal definitions of terrorism often **exclude state actors** or state sponsors

Defining “Extremism”

Extremism is **context-dependent** — it describes a deviation from something ‘ordinary’ or ‘mainstream’:

- **Relativistic**: a belief system outside the bounds of currently acceptable mainstream norms
- **Non-relativistic**: a belief system held together by unwavering hostility toward a specific **out-group**
- **Violent extremism**: “vocal or active opposition to fundamental values, including democracy, the rule of law, individual liberty, and mutual respect and tolerance” (UNODC 2021)
- **Online extremism**: internet activism related to, engaged in, or perpetrated by groups holding doctrinally extremist views (Winter et al. 2020)

Types of Extremism and Terrorism

- **Traditional (offline → online)**: Right Wing, Left Wing, Religious, Separatist, Single-Issue
- **Traditional ideology emerging online**: Manosphere, Trans-Exclusionary Radical Feminists (TERFs), Groypers
- **Hybridized / Mixed-Unclear-Unstable (MUU)**: Involuntary Celibates, Ecofascism, Tradwives, Nihilistic Violence
  - "Post-organizational" — leaderless, grassroots, *merges* disparate grievances
  - Example: **Devon Arthurs** — Atomwaffen leader, self-described "Salafist National-Socialist"
  - Example: **Ethan Melzer** — US soldier who facilitated a jihadist ambush on his own unit while engaged with neo-Nazi, Satanist, and O9A material

Davey et al. 2021 (ISD); Jones & Comerford 2023; Brace, Baele, & Ging 2024.

Nihilistic Violent Extremism (NVE)

Background

- A violent scene growing since the **second half of the 2010s**
- Members reject civil-society values, hold a **misanthropic worldview**, communicate primarily online, internationally networked
- **Officially classified** and utilized as a specific threat category by the FBI primarily from **early 2025** onward

Key characteristics

- **Misanthropy** — universal hatred and disillusionment with society
- Seeks **societal collapse**, destruction, and chaos
- Prioritizes **spectacle, notoriety, and aestheticized violence** over coherent ideology
- Expands primarily across online ecosystems (e.g., the COM Network)

Hart (2026); Neumann (2026) / Konrad Adenauer Foundation.

Five-minute exercise

Get in teams of 3-4

In pairs, draft workable definitions for:

1. **Extremism** for your fictional online platform's community standards
2. **Terrorism** for your fictional online platform's community standards

Use examples to illustrate the types of content and behavior you are seeking to prohibit.

Radicalization Online

Radicalization Online

- The internet plays an **increasingly important** role in radicalization pathways
- Key online mechanisms: **facilitation**, **echoing**, sometimes **acceleration**
- Most radicalization is shaped by **hybrid** constellations of online and offline factors
- Increased **glorification of terrorism** on platforms like TikTok

Kenyon, Binder, & Baker-Beall (2022) — *Ministry of Justice.* Mølmen & Ravndal (2021).

Process of Radicalization: the 3N model

- **Need** — quest for significance; motivation to restore it when lost
- **Narrative** — ideological framework that justifies action
- **Network** — community of like-minded others that validates the narrative

The 3N model treats radicalization as the joint product of these three determinants acting on attitudes, intentions, and behavior.

Kruglanski, Bélanger & Gunaratna (2019). *The three pillars of radicalization: Needs, narratives, and networks.* Oxford University Press.

Need

“Quest for significance” — the universal need to be recognized and respected by people who matter.

- When significance is **lost**, individuals become motivated to **restore** it
- Precipitating factors: religious upbringing, low integration, criminal history, drug use, psychopathy, dominance orientation, disconnectedness, low self-control, low life attachment, mental health, job loss, anger

Wolfowicz et al. (2020, 2021) — systematic reviews of radicalization risk/protective factors.

Narrative

Ideological framework that determines actions to realize significance and provides moral justification.

- Ideological narratives of the culture in which the individual is embedded
- Examples: grievances, anti-democracy, moral neutralization, segregation, collective relative deprivation, misogyny, authoritarianism, fundamentalism, exposure to violence, “red-pill” content, anti-establishment

Network

Like-minded others who validate and reinforce the collective narrative.

- People are motivated to seek the presence of others who share similar beliefs
- Examples: in-group superiority, similar peers, online posting, deviant peers, military service (current or past), online contact with radicals, online gaming environments

Countermeasures: Law and Regulation

Countering online extremism — Europe

EU Rules on Terrorist Content Online (TCO, 2021/784) — since June 2022

- All tech companies offering services in the EU must act against terrorist content
- Hosting providers must **remove terrorist content within 1 hour** of a removal order
- Non-compliance liable for fines up to **4% of global turnover**

EU Digital Services Act (DSA) — since Nov. 2022

- Online platforms must remove content illegal in any EU Member State, suspend accounts disseminating illegal content, and report criminal behavior
- Very Large Online Platforms produce annual risk assessments, undergo independent audits, have risk-mitigation measures, and appoint a compliance officer

Assessment (2026): TCO is actively used by authorities — high platform compliance but risks of over-removal and free-expression concerns. DSA has increased platform transparency but enforcement varies strongly between Member States, with limited impact on borderline content.

Countering online extremism — United States

Federal law

- US Anti-Terrorism Act (ATA)
- Justice Against Sponsors of Terrorism Act (JASTA)

Key Supreme Court cases

- **Gonzalez v. Google LLC** — does § 230 exempt platforms when they *algorithmically promote* terrorist content?
- **Twitter, Inc. v. Taamneh**
- **Moody v. NetChoice LLC**
- **NetChoice LLC v. Paxton**

→ The US federal government does **not (yet) directly regulate** online platforms for extremist content; § 230 plus First Amendment pre-empt most state-level attempts.

How anti-extremism laws can be weaponized against human rights

Minneapolis, US — Jan. 2026
“Just hours after federal agents shot and killed a 37-year-old man in Minneapolis, Trump administration officials called the deceased a ‘would-be assassin’ and blamed Democrats for siding with ‘terrorists.’ ”

Berlin, Germany — May 2024
“Five members of *Letzte Generation*, Germany’s equivalent to Just Stop Oil, have been charged with ‘forming a criminal organisation,’ a move civil-rights campaigners say could in effect criminalise future support.”

London, UK — June 2025
“The protest group Palestine Action does not promote violence against people. But after it damaged military property, the British government banned it as a terrorist organization.”

Countermeasures: Platforms

The role of platforms

Reactive / defensive

- Content removal
- Account suspensions
- Counter-speech / counter-activism

Proactive / offensive

- Redirect method
- Awareness-raising / education

Online counter-radicalization uses a range of **content-moderation tools**. The global market for these technologies is growing rapidly — projected from **US$9.8B** today to over **US$32B by 2031** (Bloomberg 2022).

Goldman, E. (2021). "Content Moderation Remedies," *Michigan Technology Law Review.*

Content and Account Removal

Hash-Sharing Database — GIFCT (Global Internet Forum to Counter Terrorism)

- Identify and remove terrorist or violent extremist content, and the producers of that content
- Uses **hashes** to uniquely identify problematic content; platforms upload hashes to a shared database
- Complemented by labels (content type, producing entity, behavioral elements)
- Other platforms use the database to identify and remove matching content on their services

Knowledge Sharing Platform — Tech Against Terrorism (TAT)

- Resources for **smaller** tech companies to implement effective, human-rights-compliant counter-terrorism responses
- Identifies and alerts on terrorist content, users, and groups — especially on smaller file-sharing and web-archiving sites

*Platforms publish policies on this kind of content — see Meta, YouTube, TikTok, and X policy

Counter Speech

Any **direct response** to hateful or harmful speech that seeks to undermine it.

Types of counter speech

- Presenting facts to correct misstatements or misconceptions
- Pointing out hypocrisy or contradictions
- Warning of offline or online consequences
- Denouncing hateful or dangerous speech

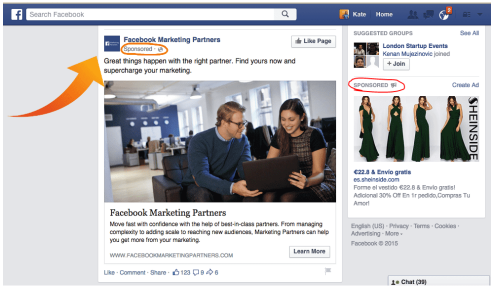
Goal and target

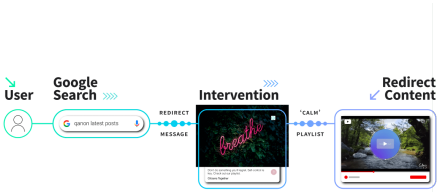
- The "**moveable middle**" and "interpreters"
- Encourage others to join the conversation and be supportive
- Prevent further spread of the dangerous message

Redirect Method

The **Redirect Method** uses targeted advertising to connect people searching online for harmful content with constructive alternative messages.

- Similar to targeted advertising
- Users are **categorized by what they search** online
- Profiles are identified and targeted with **counter messages**





Criticizing current countermeasures

- Regulators and tech firms have been criticized for **shirking responsibilities** and lacking a coordinated response
- **Example**: In Oct. 2025, a UK parliamentary committee criticized both regulators and platforms for failing to adequately respond to online harms that contributed to real-world riots in summer 2024
- Countermeasures can produce **side effects**:
  - Ostracize minorities
  - Inadvertently promote extremist content (Streisand effect)
  - Enable trolling via mass-flagging
  - Push users to fringe platforms
  - Evade public oversight
- **Technological fetishism** (“AI will fix this”) vs. digitizing traditional countermeasures

Challenges and Risks

Challenges

- Scale, speed, the “grey zone”
- Misclassification and bias
- Hyper-localization of extremism; globally operating platforms; no consensus definitions
- Adaptation and migration of extremists
- Transparency and oversight vs. insight

Risks

- Violating **civil liberties**: privacy, freedom of thought, freedom of association

Trends in (Counter-) Radicalization, Terrorism, and Extremism

Countermeasures — safety by design, decentralized content moderation, middleware, multi-stakeholder governance, AI with human-in-the-loop.

Radicalization / Terrorism / Extremism — encrypted messaging, gaming platforms, metaverse, DWeb (decentralized web), AI-produced propaganda and deepfakes, fintech / crypto fundraising, satellite internet and drones, grassroots diversification.

Case Studies

Case study: January 6 insurrection

What role did online platforms play in the January 6, 2021 storming of the Capitol?

Are companies and law enforcement (better) prepared to confront similar threats today?

Case study: Online gaming

- **Far-right and jihadist actors** have used gaming-related spaces for propaganda, recruitment, and mobilization
- Extremist actors **mod** established games popular with young users (e.g., Roblox) to embed ideology
- Countering this requires:
  - Better moderation in gaming platforms
  - Safety-by-design features
  - Stronger community norm-setting

Lamphere-Englund, G. & White, J. (2023). *The online gaming ecosystem: Assessing digital socialisation, extremism risks and harms mitigation efforts.* Global Network on Extremism and Technology.

Summary

Summary

- **Concepts**: radicalization, terrorism, and extremism are each contested
- **Internet's role**: augments — does not simply host — extremism
- **No universally accepted definitions** → politicization and enforcement inconsistency
- **Digital technologies accelerate** radicalization in combination with offline processes
- **Countermeasures** face real trade-offs:
  - Reactive (removal) vs. proactive (counter-speech, redirect)
  - Must comply with **international human rights** standards
  - Large potential for improvement, but real risks of over-removal and liberty-chilling